WHAT IS CLAIMED IS:

1. A cryptographic communication method wherein when different encryption algorithms are operated at a transmission side and a reception side, the transmission side encrypts an encryption algorithm operated at the transmission side with an encryption algorithm operated at the reception side and transmits the encrypted algorithm to the reception side.

2. A cryptographic communication method wherein information on an encryption algorithm operated at a transmission side and information on an encryption algorithm operated at a reception side are obtained from the transmission side and when different encryption algorithms are operated at the transmission side and the reception side, an encryption algorithm operated at the transmission side is encrypted with an encryption algorithm operated at the reception side and transmitted to the reception side.

3. A cryptographic communication method as claimed in claim 2 wherein signature data produced based on a public key preliminarily allocated to the transmission side is supplied to the reception side with said encrypted encryption algorithm.

4. A cryptographic communication method as claimed in claim 2 wherein signature data produced based on a public key preliminarily allocated to the transmission side is supplied to the transmission side together with said encrypted encryption algorithm and transmitted to the reception side.

5. An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side; and

querying a data base in which a correspondence between the user identifier indicating the user and an encryption algorithm operated by the user is preliminarily described about each user and then retrieving the encryption algorithm operated by the user of the transmission side and the encryption algorithm operated by the user of the reception side,

wherein if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, data indicating the encryption algorithm operated by the user of the transmission side is encrypted with the encryption algorithm operated by the user of the reception side and

transmitted to the user of the reception side.

6. An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side;

querying a data base in which a correspondence between user identifier indicating the user, an encryption algorithm operated by the user and an encryption key is preliminarily described about each user so as to obtain the encryption algorithm operated by the user of the transmission side and an encryption key thereof and an encryption algorithm operated by the user of the reception side and encryption key thereof,

wherein if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, data indicating the encryption algorithm operated by the user of the transmission side and encryption key produced based on the encryption key operated by the user of the reception side corresponding to a key length of the encryption algorithm is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side.

7. An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side; and

querying a data base in which a correspondence between user identifier indicating the user, an encryption algorithm operated by the user and an encryption key is preliminarily described about each user so as to obtain the encryption algorithm operated by the user of the transmission side and an encryption key thereof and the encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and data obtained by encrypting the encryption algorithm operated by the user of the transmission side with the encryption algorithm operated by the user of the reception side and signature data produced for the encryption key operated by the user of the reception side are transmitted to the user of the reception side.

8. An encryption algorithm sharing management method for sharing the encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side; and

querying a data base in which a correspondence between the user identifier indicating the user, an encryption algorithm operated by the user and an encryption key is preliminarily described about each user so as to obtain the encryption algorithm operated by the user of the transmission side and an encryption key thereof and an encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and data indicating the encryption algorithm operated by the user of the transmission side and encryption key produced based on the encryption key operated by the user of the reception side corresponding to a key length of the encryption algorithm is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of

the reception side with the signature data produced corresponding to the encryption key operated by the user of the reception side.

9. Network communication system composed by connecting a plurality of users, comprising at least an encryption key management station to be connected from a user of a transmission side,

said encryption key management station obtaining, from the user of the transmission side, information indicating an encryption algorithm operated by the user and information indicating the encryption algorithm operated by the user of the reception side and if different encryption algorithms are operated by users of the transmission side and a reception side, encrypting the encryption algorithm operated by the user of the transmission side with an encryption algorithm operated by the user of the reception side and transmitting it to the user of the reception side.

10. Network communication system composed by connecting a plurality of users, comprising at least an encryption key management station to be connected from a user of a transmission side,

said encryption key management station comprising a data base in which a correspondence between a user identifier indicating a user and an encryption algorithm

operated by the user is preliminarily described about each user;

wherein

when a communication is carried out from the user of the transmission side to a user of a reception side, a user identifier indicating the user and a reception side user identifier are obtained from the user of the transmission side and said data base is queried with the obtained identifier as a key so as to obtain an encryption algorithm operated by the user of the transmission side and an encryption algorithm operated by the user of the reception side, and

if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, the encryption algorithm operated by the user of the transmission side is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side.

11. An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side;

querying a data base in which a correspondence between the user identifier indicating the user and an encryption algorithm operated by the user is preliminarily described about each user so as to retrieve an encryption algorithm operated by the user of the transmission side and an encryption algorithm operated by the user of the reception side; and

if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, data indicating the encryption algorithm operated by the user of the transmission side is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side.

12. An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side; and

querying a data base in which a correspondence between the user identifier indicating the user, an encryption algorithm operated by the user and an encryption key thereof is preliminarily described about each user so as to obtain the encryption algorithm operated by the user of the

transmission side and an encryption key and the encryption algorithm operated by the user of the reception side and an encryption key,

wherein if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, data indicating the encryption algorithm operated by the user of the transmission side and the encryption key produced based on the encryption key operated by the user of the reception side corresponding to a key length of the encryption algorithm is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side.

13. An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side; and

querying a data base in which a correspondence between the user identifier indicating the user, an encryption algorithm operated by the user and an encryption key is preliminarily described about each user so as to obtain the encryption algorithm operated by the user of the transmission side and an encryption key thereof and the

encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and the encryption algorithm operated by the user of transmission side is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side with the signature data produced for the encryption key operated by the user of reception side.

14. An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side; and

querying a data base in which a correspondence between the user identifier indicating the user, an encryption algorithm operated by the user and an encryption key is preliminarily described about each user so as to obtain the encryption algorithm operated by the user of the transmission side and an encryption key thereof and the

encryption algorithm operated by the user of the reception side and an encryption key thereof,

wherein if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, signature data produced for the encryption key operated by the user of the transmission side is transmitted to the user of the transmission side and data indicating the encryption algorithm operated by the user of the transmission side and the encryption key produced based on the encryption key operated by the user of the reception side corresponding to a key length of the encryption algorithm is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side with signature data produced corresponding to the encryption key operated by the user of the reception side.

15. Network communication system composed by connecting a plurality of users, comprising at least an encryption key management station to be connected from a user of a transmission side,

said encryption key management station obtaining, from the user of the transmission side, information indicating an encryption algorithm operated by the user and information indicating an encryption algorithm operated by

a user of a reception side, and when different encryption algorithms are operated by the user of the transmission side and the user of the reception side, encrypting the encryption algorithm operated by the user of the transmission side with the encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side.

16. Network communication system composed by connecting a plurality of users, comprising at least an encryption key management station to be connected from a user of a transmission side, said encryption key management station comprising a data base in which a correspondence between a user identifier indicating a user and an encryption algorithm operated by the user is preliminarily described about each user;

wherein

when a communication is carried out from the user of the transmission side to a user of a reception side, a user identifier indicating the user and a reception side user identifier are obtained from the user of the transmission side, and said data base is queried with the obtained identifier as a key so as to obtain an encryption algorithm operated by the user of the transmission side and an encryption algorithm operated by the user of the reception side, and

if the encryption algorithm operated by the user of the transmission side is different from the encryption algorithm operated by the user of the reception side, the encryption algorithm operated by user of transmission side is encrypted with the encryption algorithm operated by the user of the reception side and transmitted to the user of the reception side.

17. A cryptographic communication method wherein if different encryption algorithms are operated by a transmission side and a reception side, an encryption algorithm operated by the reception side is encrypted with an encryption algorithm operated by the transmission side and transmitted to the reception side.

18. A cryptographic communication method wherein information indicating an encryption algorithm operated by a transmission side and information indicating an encryption algorithm operated by a reception side are obtained from the transmission side and when different encryption algorithms are operated by the transmission side and the reception side, the encryption algorithm operated by the reception side is encrypted with the encryption algorithm operated by the transmission side and transmitted to the transmission side.

19. A cryptographic communication method as claimed in claim 18 wherein signature data produced based on a public key preliminarily allocated to the reception side is supplied to the transmission side with the encrypted encryption algorithm.

20. An encryption algorithm sharing management method for sharing an encryption algorithm for cryptographic communication, comprising the steps of:

from a user of a transmission side, obtaining a user identifier indicating the user and a user identifier indicating a user of a reception side;

querying a data base in which a correspondence between the user identifier indicating the user and an encryption algorithm operable by the user is preliminarily described about each user so as to obtain an encryption algorithm operable by the user of the transmission side and an encryption algorithm operable by the user of the reception side;

determining whether or not there is an encryption algorithm operable by the user of the transmission side and the user of the reception side commonly; and

if the commonly operable encryption algorithm exists, it is notified the user of the transmission side that cryptographic communication at the user of the transmission side and the user of the reception side is enabled.

21. An encryption algorithm sharing management method as claimed in claim 20 wherein:

if the commonly operable encryption algorithm exists, information indicating the encryption algorithm is transmitted to the user of the transmission side and

if the commonly operable encryption algorithm exists, it is notified the user of the reception side that cryptographic communication at the user of the transmission side and the user of the reception side is disabled.

22. An encryption algorithm conversion method for converting an operating first encryption algorithm to other second encryption algorithm comprising:

querying a data base in which a correspondence between a user identifier indicating a user, an encryption algorithm operated by the user and an encryption key is preliminarily described with a user whose encryption algorithm is to be converted with a key so as to obtain a first encryption algorithm operated by the user and a first encryption key; and

with a first management secret key preliminarily allocated for management and operated on the first encryption algorithm, supplying first and second signature data written in the first and second encryption keys, public key data obtained by encrypting a second public key corresponding to a second management secret key operated on

the second encryption algorithm preliminarily allocated for management with the first encryption algorithm, a second encryption algorithm encrypted with the first encryption algorithm and signature data produced based on the second management secret key to the user.